Claims

I claim:

1. A device for digital signature of an electronic document by means of a signature creation unit, which is portable and in the form of a card and protected against manipulation,

which is planned for cooperation with a data processing unit for providing the electronic document to be signed and for receiving the digital signature,

and which is constructed to deposit the secret, hacker-protected private digital signature encryption, where through a signature processor unit of the signature creation unit the digital signature can be produced on the basis of a signage string characteristic for the electronic document as well as the private digital signature encryption,

characterized by,

the signature creation unit showing an output unit for giving an output signal for a user of the data processing unit, which cannot be influenced by the data processing unit,

an input unit being associated with the signature creation unit, which can be confirmed by the user, and

the signature creation unit being formed in such a way, that as a response to the output signal a user input into the input unit is required, before the digital signature is created and/or transmitted to the data processing unit.

2. A device according to Claim 1, characterized by a public digital signature encryption, provided by a certification unit preferably being connected by a data transmission network, being associated with the private signature encryption, which enables the validation of the private signature encryption by comparison of the characteristic signage string with the digital signature, to which the public digital encryption has been applied.

3. A device according to Claim 1, characterized by an output value, corresponding to the output signal and entered into the input unit by the user, being part of the electronic document and being able to be displayed with it after the digital signature was accomplished, or being a part of the output signal of the electronic document, to which the private signature encryption was applied.

4. A device according to one of the Claim 1, characterized by the input unit being a part of the card and/or module-like signature creation unit or a part of a further data processing unit, and not having a direct physical or logical connection to the data processing unit.

5. A device according to Claim 4, characterized by an output value of the output unit as output signal being able to be set or influenced by the input unit and/or the output unit being connected to the signature creation unit by means of a wireless application, especially over a microwave or light-based connection.

6. A device according to Claim 4, characterized by the input unit being constructed for reception of bio identification characteristics, especially for fingerprints, voice or retina of a user.

7. A device according to Claim 1, characterized by the input unit being physically separate from the signature creation unit.

8. A device according to Claim 7, characterized by the input unit being connected to the signature creation unit over a wireless application, especially a microwave or light-based connection.

9. A device for digital signature of an electronic document by means of a signature creation unit, which is portable and in the form of a card and protected against manipulation,

which is planned for cooperation with a data processing unit for providing the electronic document to be signed and for receiving the digital signature and which is constructed to deposit the secrete, hacker-protected private digital signature encryption, where through a signature processor unit of the signature creation unit the digital signature can be produced on the basis of a signage string characteristic for the electronic document as well as the private digital signature encryption,

characterized by,

the signature creation unit being formed for storage of a number of private signature encryptions for the same signature process, and the signature creation unit having a selection unit for selection of one of the numbers of private digital encryptions before creating the digital signature, where the selection unit executes the selection as response to one of the digital parameters provided by a parameter storage unit.

10. A device for digital signature of an electronic document by means of a signature creation unit, which is portable and in the form of a card and protected against manipulation,

which is planned for cooperation with a data processing unit for providing the electronic document to be signed and for receiving the digital signature and which is constructed to deposit the secrete, hacker-protected private digital signature encryption, where through a signature processor unit of the signature creation unit the digital signature can be produced on the basis of a signage string characteristic for the electronic document as well as the private digital signature encryption,

characterized by,

the signature creation unit being formed for parameter-controlled application of at least one private digital signature encryption a number of times to the characteristic signage string and/or further signage strings, which are dependent on it or connected to it, where the operating parameters controlling the application provided by an operating parameter storage unit can be generated from data of the electronic document or by a time signal unit or can be input or output externally

and a result of the parameter-controlled application can be inserted into a data range of the electronic document before a concluding signing.

11. A device according to Claim 10, characterized by a public signature encryption, provided by a certification unit preferably over a data transmission network, being associated with each of a number of private signature encryptions, which enables a validation of the private digital signature encryption by comparison of the characteristic signage string with the digital signature, to which the public signature encryption has been applied.

12. A device according to Claim 10, characterized by the digital parameter being selected or determined in a time dependent way and a corresponding time signal being able to be produced either by a time stamp unit of the signature creation unit or by an external timer.

13. A device according to Claim 12, characterized by the digital parameter and the time signal being deposited and available for validation purposes on an external server unit, preferably connected over a data transmission network, where the server unit reacts as response to a validation inquiry concerning a digital signature with a confirmation signal, without providing the digital parameter to the inquirer.

14. A device according to Claim 11, characterized by the signature creation unit having means for deleting of such digital parameters, which have a time dependency to the past for the deletion point.

15. A device for digital signature of an electronic document by means of a signature creation unit, which is portable and in the form of a card and protected against manipulation,

which is planned for cooperation with a data processing unit for providing the electronic document to be signed and for receiving the digital signature

and which is constructed to deposit the secrete, hacker-protected private digital signature encryption, where through a signature processor unit of the signature creation unit the digital signature can be produced on the basis of a signage string characteristic for the electronic document as well as the private digital signature encryption,

characterized by,

means being provided for deposit of the digital signature together with an objective time signal and especially with further data in a signature status server unit preferably connected over an electronic data transmission network, which is protected against manipulation and formed as a storage unit.

16. A device according to Claim 15, characterized by a public digital signature encryption being associated with the private digital signature encryption, provided by a certification unit preferably connected over a data transmission network, which allows a validation of the private digital signature encryption by comparison of the characteristic signage string with the digital signature, to which the public signature encryption has been applied.

17. A device according to Claim 16, characterized by the signature creation unit being formed for additional availability of original data of the electronic document, of compromised or encrypted original data or of structural data associated with the original data, where preferably means for access are provided for this purpose.

18. A device according to Claim 1, characterized by a time stamp unit as part of the encryption creation unit, which is provided for producing a digital time signal or for means for receiving a digital time signal and for adding the digital time signal, signed by the digital private encryption, to the electronic document before signing.

19. A device according to Claim 1, characterized by a text construction unit as part of the encryption creation unit, which is provided for the creation of digital text addition and for adding the means of the digital text addition, signed by means of the digital private encryption, to the electronic document before signing.

20. A device according to Claim 15, characterized by the means for storing of the digital signature and especially of further data, preferred parameters or time signals being able to be executed on the signature status server unit by the signature creation unit or by the data processing unit, or being executed over structure or metadata within the document as instructions to a document administration unit.

21. A device according to Claim 15, characterized by the signature status server unit reacting in response to a validation inquiry regarding a digital signature with a confirmation signal, without making the digital parameter stored on the server unit available to the inquirer.

22. A device according to Claim 9, characterized by the digital parameters being a calculated document-range specific function, especially applied to segments of an electronic document by an individual signature encryption or a parameter-controlled application of a pre-determined series of signature encryptions, where the document-range specific application is executed by parameter control.